Kas ir sociālā inženierija?

Cilvēku neapdomība mēdz būt bezgalīga, no viņiem var izmakšķerēt jebkuru informāciju, un viņi spēj paveikt vismuļķīgākās darbības. Pēc Latvijas piemēriem labi zinām, ka joprojām un vēl aizvien atrodas indivīdi, kurus var apmānīt ar SMS.

Ar terminu ”Sociālā inženierija” saprot zinātni par manipulēšanu ar cilvēku, tā attieksmi un reakciju uz konkrētu situāciju ar galveno mērķi panākt sensitīvas. Sensitīva informācija ir informācija, kuru persona uzskata par aizsargājamu, jo tās neatļauta izmainīšana, bojāšana, atklāšana vai zaudēšana var būt postoša.

Sociālās inženierijas paņēmieni un mērķi var būt visdažādākie un šāda veida uzbrukumi ļoti bieži notiek gan internetā, gan telefoniski, kā arī aci pret aci.

Uzbrucēji bieži vien izmanto cilvēku dabisko vēlmi būt izpalīdzīgiem, kā arī viņu ziņkārību.

Tiešsaistē izmantotie paņēmieni visbiežāk ir šādi:

* e-pasta pielikumaatsūtīšana, kurā ir kāda interesanta informācija vai reklāma;
* situācijas izspēlēšana, uz kuru reaģējot, cilvēks izpauž privātu informāciju.

Dzīvē šie paņēmieni var vēl vairāk variēties.

Sociālā inženierija ir plaša un daudzveidīga, tās scenāriji un situācijas atkarīgi no uzbrucēja izdomas un uzbrukuma mērķa.

Sociālās inženierijas uzbrukumā var ietilpt tādas klasiskas metodes kā viltus telefona zvans, viltus e-pasts jeb pikšķerēšana (no angļu valodas –*phishing*), kā arī inficētu datu nesēju izplatīšana, atkritumu inspicēšana (*dumpster diving*) vai pat fiziska piekļuve. Svarīgi, ka pie parolēm var tikt arī, ja noskatās lietotājvārdu un paroles (redz taustiņu spiešanu, noskatās pār plecu).

Izlikšanās par citu personu, izmantojot iepriekš sagatavotu scenāriju. Piemēram, upuris pa telefonu izpauž savu datorsistēmas lietotāja vārdu un paroli vai ielaiž telpās svešu cilvēku, noticot, ka tas ir jaunais kolēģis vai kāds ārpakalpojuma sniedzējs.

Iedot «ēsmu» un panākt, lai cilvēks atver e-pasta pielikumu vai saiti (noformējot e-pastu kā reklāmu, brīdinājumu vai citu maldinājumu) vai izmanto nejauši atrastu USB zibatmiņu, ko atverot ielādējas kaitnieciska programmatūra un sniedz krāpniekam piekļuvi šī cilvēka datorsistēmās esošajiem datiem. Tieši šī metode izmantota krāpniecisko e-pastu gadījumā, kas šobrīd tiek izsūtīti lielu un zināmu Latvijas organizāciju vārdā.

Panākt, lai lietotājs pats ievada sensitīvus datus kādā tīmekļa formā, caur kuru informācija nonāk tieši pie krāpnieka.

# Eksperta ieteikumi aizsardzībai pret uzbrukumiem internetā[[1]](#footnote-1)

Tikai zinošs interneta lietotājs ir pasargāts. Informētība ir galvenais ierocis cīņā ar sociālās inženierijas apdraudējumu. Regulāri jāatgādina, kuri dati tiek klasificēti kā konfidenciāli, kā ar tiem jārīkojas un kādas ir drošības prasības, procedūras darbā ar sensitīviem datiem.

Svarīgs priekšnoteikums ir arī regulāra izglītošanās.

Lai pasargātu personīgos datus virtuālajā vidē, ir jābūt informētiem par potenciālajiem apdraudējumiem un jāievēro piesardzība. Piemēram, jāizmanto šifrēts bezvadu interneta pieslēgums darbam ar datoru sabiedriskās vietās.

Nedrīkst paļauties uz acīmredzamo, piemēram, jāpārbauda arī pie paša durvīm klauvējoša policijas darbinieka identitāte.

Jāņem vērā, ka telefona zvani un e-pasti nav paredzēti konfidenciālas informācijas nodošanai. Tam paredzēti citi kanāli un informācijas nesēji.

Sociālās inženierijas uzbrukumi lielākoties ir ļoti pārliecinoši, tāpēc cilvēkam ir jāsaglabā modrība un uzmanība, kā arī par aizdomīgiem gadījumiem jāziņo atbildīgajām instancēm.

Ievērojot drošības priekšnosacījumus virtuālajā vidē, iespējams pasargāt sevi, jo sociālā inženiera uzdevums būs kļuvis daudz sarežģītāks un krāpnieki vērsīsies pie tiem, kuri vēl nav paspējuši parūpēties par savu drošību.

**Uzbrucēju komunikāciju veidi:**

* personīgi kontakti;
* tālrunis;
* elektroniskais pasts;
* ļaundabīga programma.

**Aizsardzības stratēģija skolā:**

* darbojošies IT drošības noteikumi;
* stingra piekļuves procedūra IT resursiem ar lietotājvārdu un paroli;
* stingra paroļu izveidošanas procedūra;
* lojālas un draudzīgas darba vides izveidošana;
* procedūra, kā un kam paziņot par incidentu.

**Rīcība drošības incidenta un pārkāpumu gadījumos:**

* pats atbildīgs par sava datora drošību;
* jānovērtē kaitējums, un jāinformē vēcāki;
* portālā www.esidross.lv var meklēt padomus, kā risināt problēmas un kā aizsargāt savu informāciju nākotnē.

Kas ir ļaunprogrammatūra?

Ļaunprogrammatūra ir ļaunprātīga programmatūra — programma vai datne, kas ir īpaši izstrādāts ar mērķi bojāt sistēmu vai traucēt tās darbību. Kā piemēru var nosaukt vīrusu, tārpu vai Trojas zirgu. Izmantojot dažādus pakalpojumus internetā, par bīstamām saitēm var tikt paziņots, ka no vietnes var tikt lejupielādēta ļaunprātīga programmatūra, kas var kaitēt jūsu datoram.

Vietne var tikt atzīmēta kā kaitīga, ja indeksēšanas laikā tiek konstatēts, ka kādā no vietnes lapām ir ietverts kaitīgs saturs. Ar kaitīgu saturu šajā gadījumā saprot ļaunprātīgas programmatūras lejupielādi jūsu ierīcē.

Pēc vikipēdijas lapas apraksta[[2]](#footnote-2), Ļaunprogrammatūra ([angļu](https://lv.wikipedia.org/wiki/Ang%C4%BCu_valoda): malicious software, malware) ir [programmatūra](https://lv.wikipedia.org/wiki/Programmat%C5%ABra), kas tiek izmantota, lai traucētu [datora](https://lv.wikipedia.org/wiki/Dators) darbību, ievāktu slepenu informāciju, piekļūtu privātām [datorsistēmām](https://lv.wikipedia.org/w/index.php?title=Datorsist%C4%93ma&action=edit&redlink=1), bojātu datorsistēmu bez tās lietotāja piekrišanas. Ļaunprogrammatūra var parādīties kā [izpildāmais kods](https://lv.wikipedia.org/w/index.php?title=Izpild%C4%81mais_kods&action=edit&redlink=1), [skripts](https://lv.wikipedia.org/w/index.php?title=Skripts&action=edit&redlink=1), aktīvais saturs vai cita programmatūra.

Ļaunprogrammatūra var būt slepena, kas paredzēta, lai nozagtu informāciju vai izspiegotu datorlietotājus ilgāku laika periodu, viņiem pašiem to nezinot, tā var būt arī paredzēta kaitējuma nodarīšanā. Pie ļaunprogrammatūras pieder [datorvīrusi](https://lv.wikipedia.org/wiki/Datorv%C4%ABruss), [tārpi](https://lv.wikipedia.org/w/index.php?title=Datort%C4%81rps&action=edit&redlink=1), [Trojas zirgi](https://lv.wikipedia.org/wiki/Trojas_zirgs_%28datorika%29), [spiegprogrammatūras](https://lv.wikipedia.org/w/index.php?title=Spiegprogrammat%C5%ABra&action=edit&redlink=1), [reklāmprogrammatūras](https://lv.wikipedia.org/wiki/Rekl%C4%81mprogrammat%C5%ABra) un citas ļaunprātīgas programmatūras. Saskaņā ar 2011. gada datiem lielākā daļa ļaunprogrammatūras bijuši tārpi vai Trojas zirgi, nevis vīrusi.

Ar terminu "ļaunprogrammatūra" tiek apzīmēta vienīgi tā programmatūra, kas apzināti nodara kaitējumu. Ja programmatūra kaitējumu rada kļūdu vai sliktas izstrādes dēļ, tad tā netiek klasificēta kā ļaunprogrammatūra. Parasti lietotāji un organizācijas, mēģinot aizsargāties pret ļaunprogrammatūras uzbrukumiem, lieto dažādu programmatūru, piemēram, pretvīrusu programmu vai [ugunsmūri](https://lv.wikipedia.org/wiki/Ugunsm%C5%ABris).

# Vai viss ir labs e-vidē?

Ar vārdu „kibernoziedznieks” parasti saprot speciālistu, kas piedalās organizētā digitālo noziegumu veikšanā grupā. Var arī teikt, ka šo cilvēku mērķis ir nelikumīgu darbību rezultātā digitālajā vidē gūt peļņu.  Nereti plašāka sabiedrība jaucās, jo uzskata, ka kibernoziedznieki ir tie paši hakeri. Hakeri (specializējas sistēmu uzlaušanā), ir tikai viens no kibernoziedznieku paveidiem, līdzās citiem. Piemēram, krāpniekiem („*fraudsters*” – veido krāpnieciskus paņēmienus, izmanto spama un „*pfishing*” metodes), kasieriem („*cashiers*” jeb banku, kredītkaršu kontu sagādnieki), līderiem (pietuvinātie pie reālās kriminālās pasaules, projektu, uzņēmumu vadītāji), „naudas mūļiem” („*money mules*”), programmētājiem (rada ļaundabīgus kodus), IT ekspertiem un citiem.

Kibernoziedznieki, kuri ir specializējušies naudas pelnīšanā, izmantojot izspiedējvīrusus, ir nolūkojuši vēl vienu auditoriju, kura pēc viņu domām būtu gatava šķirties no izpirkuma maksas. Tagad laiks ir pienācis datorspēļu faniem, kuru digitālās vērtības var tikt “sagūstītas”. Ļaunprogrammatūra ir notēmēta uz dažādām spēlēm, ieskaitot, piemēram, Call of Duty, World of Warcraft, Minecraft un World of Tanks. Programma meklē spēlētāju profilus, kartes, saglabātās spēles un to modifikācijas. Lai ļaunprogrammas upuris atgūtu kontroli pār savām iesāktajām spēlēm, viņam tiek piedāvāts samaksāt no konkrētu naudas summu, atkarībā no maksāšanas veida. Neapdomīgie to arī veic!

Kibernoziegumi

Par kibernoziegumu sauc noziegumu, kas veikts informācijas pārraides procesā. Tādi ir, piemēram, dažādi viltojumi, ko izdara, strādājot tiešsaistes režīmā. **Datornoziegums** — jebkura ar likumu aizliegta krimināli sodāma darbība vai bezdarbība, kur dators vai datortehnoloģijas produkti (datori, skeneri, drukas iekārtas, datorprogrammas, komunikācijas līdzekļi u.c.) izmantoti kā nozieguma priekšmets vai nozieguma rīks ar mērķi ietekmēt datorsistēmu tehniskos un informācijas resursus.

Datornoziegumus var iedalīt divās lielās grupās:

* noziegumi, kuri saistīti ar iejaukšanos datoru darbībā;
* noziegumi, kuros datori tiek izmantoti kā nozieguma priekšmets.

Pasaulē pašreiz dominē trīs termini, kādos nosacīti iedala datornoziegumus:

* datornoziegumi (*computercrimes*);
* ar datoriem saistīti noziegumi (*computer – related crimes*);
* kibernoziegumi (*cybercrimes*).

# Datornoziegumu veidi

Datornoziegumiem, kuri saistīti ar iejaukšanos datora darbībā ir ļoti plašs klāsts. Izplatītākie ir:

1. Nesankcionēta piekļūšana informācijai. Šādas informācijas iegūšana var būt mantkārīgos nolūkos, lai nelikumīgi iegūto informāciju tālāk pārdotu, gan vēlme pārbaudīt savas spējas, cenšoties apiet aizsardzības sistēmas.

2. “Loģisko bumbu” ievadīšana programmnodrošinājumā. Programma, kas sāk veikt ieprogrammēto uzdevumu pie attiecīgu priekšnoteikumu iestāšanās.

3. Datorvīrusu izstrāde un izplatīšana.

4. Noziedzīga nevērība izstrādājot, izgatavojot un lietojot programmvadāmas ierīces, kas noved pie smagām sekām. Neuzmanība ir līdzīga nevērībai, kas saistītas ar tehniku, transportu.

5. Informācijas viltošana. Patiesās informācijas vietā tiek sniegta nepatiesa informācija.

6. Informācijas zādzība. Ja tiek nolaupīta kāda materiāla vērtība, tad var konstatēt tās pazušanu, bet datorinformācijas jomā konstatēt, labākajā gadījumā, var tikai to, ka dotā informācija ir kopēta.

# Datornoziegumi un krimināllikums

Ar datoriem saistītās reālās briesmas sākās tos saslēdzot tīklā, radot cilvēkam iespēju, neizejot no mājām, veikt darbības dažādās pasaules valstīs dažu minūšu un pat sekunžu laikā. Ja tās ir bijušas noziedzīgas darbības, tad šo noziedzīgo darbību atklāšanā jāiesaistās jau vairāku valstu tiesību sargājošām institūcijām. Attiecināms jau uz 14 gadu sasniegušu skolēnu. Savas zināšanas izmanto jēgpilni, nekaitējot citiem!

* Necenties patvaļīgi (neatļauti) piekļūt datorsistēmai!
* Neiegūsti un neizmanto programmatūru, ja neesi iegādājies, ja par to ir jāveic maksājums.
* Nebojā programmatūru.
* Neizplati vīrusus!

Kibernoziegumus var iedalīt piecās lielās grupās:

* ar nodomu izdarīti noziedzīgi nodarījumi pret datu un datorsistēmu konfidencialitāti, integritāti un pieejamību (patvaļīga piekļūšana, informācijas sistēmas darbības traucēšana, kaitīgas programmas izplatīšana utt.);
* ar datoru saistītie noziedzīgie nodarījumi (ar datoriem saistīta viltošana, datorkrāpšana utt.);
* ar saturu saistītie noziedzīgie nodarījumi (bērnu seksuālās izmantošanas materiālu izplatīšana);
* ar autortiesību un blakustiesību pārkāpšanu saistītie noziedzīgie nodarījumi;
* noziedzīgi nodarījumi, kas saistīti ar rasismu, ksenofobiju un genocīdu propagandējošu materiālu izplatīšanu automatizētās datu apstrādes sistēmās.

1. http://www.tvnet.lv/tehnologijas/nozares\_jaunumi/490114-sociala\_inzenierija\_var\_apiet\_jebkuru\_it\_drosibas\_sistemu [↑](#footnote-ref-1)
2. https://lv.wikipedia.org/wiki/%C4%BBaunprogrammat%C5%ABra [↑](#footnote-ref-2)